РАЗВИТИЕ ИНФОРМАЦИОННЫХ УГРОЗ В ПЕРВОМ КВАРТАЛЕ 2014 ГОДА

ДЭВИД ЭММ
МАРИЯ ГАРНАЕВА
ВИКТОР ЧЕБЫШЕВ
РОМАН УНУЧЕК

KASPERSKY lab

СОДЕРЖАНИЕ

ЦИФРЫ КВАРТАЛА

- По данным KSN, в первом квартале 2014 года продукты «Лаборатории Касперского» заблокировали 1 131 000 866 вредоносных атак на компьютерах и мобильных устройствах пользователей.
- Решения «Лаборатории Касперского» отразили 353 216 351 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.
- Нашим веб-антивирусом задетектировано 29 122 849 уникальных вредоносных объектов (скрипты, веб-страницы, эксплойты, исполняемые файлы и т.д.).
- Зафиксировано 81 736 783 уникальных URL, на которых происходило срабатывание веб-антивируса.
- 39% веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США и России.
- Наши антивирусные решения обнаружили 645 809 230 вирусных атак на компьютерах пользователей. Всего в данных инцидентах было зафиксировано 135 227 372 уникальных вредоносных и потенциально нежелательных объектов.

ОБЗОР СИТУАЦИИ

ЦЕЛЕВЫЕ И APT-АТАКИ

«ЛЕДЯНОЙ ТУМАН» ПРОДОЛЖАЕТ РАССЕИВАТЬСЯ

В сентябре 2013 г. мы сообщили о целевой атаке, получившей название Icefog и направленной преимущественно на пользователей в Южной Корее и Японии. Обычно APT-атаки продолжаются в течение месяцев, а то и нескольких лет – все это время с компьютеров жертв постоянно крадут данные. Однако у злоумышленников, которые стоят за Icefog, была другая тактика: они выбирали конкретную жертву, проводили точную и короткую атаку, собирали конкретную информацию и уходили с компьютера. Эта кампания по кибершпионажу началась не позже 2011 года, в ней использовалась целая серия различных версий вредоносного ПО, в том числе версия, нацеленная на Mac OS.

После публикации нашего отчета атаки Icefog прекратились и злоумышленники закрыли все известные командные серверы. Тем не менее, мы продолжали следить за ситуацией, продолжая sinkhole-операцию доменов и анализируя сетевые связи жертв. В процессе анализа мы обнаружили существование следующего поколения бэкдоров Icefog – в этот раз это была Java-версия зловреда, которую мы назвали Javafog. Анализ сетевых обращений к одному из доменов (lingdona[dot]com), подвергшихся процедуре sinkhole, показал, что клиент может быть Java-приложением; последующее расследование увенчалось тем, что был получен образец этого приложения (подробности анализа доступны здесь).

При проведении sinkhole-операции по этому домену мы отследили восемь IP-адресов, соответствующих трем уникальным жертвам Javabot. Все они находились в США; одной из них оказалась очень крупная независимая нефтегазовая компания, ведущая деятельность во многих странах. Возможно, Javafog был разработан конкретно для операции в США, которая должна была длиться не дольше типичных атак Icefog. Причиной разработки Java-версии зловреда могло стать то, что она незаметнее и ее сложнее обнаружить.

КТО СКРЫВАЕТСЯ ЗА «МАСКОЙ»

В феврале Исследовательский центр «Лаборатории Касперского» опубликовал отчет о комплексной кампании по кибершпионажу, получившей название «Маска», или Careto (в исп. сленге – «безобразное лицо», «маска»). Целью этой кампании было украсть конфиденциальные данные у разных жертв. Эти мишени представляли собой государственные учреждения, посольства, энергетические компании, исследовательские институты, частные инвестиционные компании и политических и общественных активистов и были расположены в 31 стране мира – полный список доступен здесь.

Атаки начинаются с целевого фишингового сообщения со ссылкой на вредоносный веб-сайт, содержащий эксплойты. После успешного заражения пользователя-жертву перенаправляют на легитимный веб-сайт, о котором шла речь в электронном сообщении – например, на новостной портал или на видео. В состав «Маски» входит сложный троянец-бэкдор, способный перехватывать все каналы связи и собирать все виды данных с зараженного компьютера. Как и в случае Red October и других целевых атак до него, в коде используется модульная архитектура, что позволяет создателям добавлять при необходимости новый функционал. Помимо этого, «Маска» широко раскидывает свои сети: версии бэкдора существуют для Windows и Mac OS X, а также, по некоторым данным, могут быть версии и под Linux, iOS и Android. Троянец также использует очень сложные технологии сокрытия своих действий.

Основной задачей киберпреступников, стоящих за «Маской», является кража данных с компьютеров жертв. Вредоносная программа собирает с зараженной системы данные самого разного характера: ключи шифрования, конфигурации VPN-соединений, SSH-ключи, RDP-файлы, а также неизвестные типы файлов, которые могут иметь отношение к специальным инструментам шифрования, используемым на военном и государственном уровне.

Мы не знаем, кто стоит за этой кампанией. По некоторым признакам можно предположить, что киберпреступники говорят на испанском, но такая зацепка мало что дает – этот язык используется во многих регионах. Возможно также, что эта подсказка ложная и специально дается, чтобы пустить аналитиков по ложному пути. Очень высок профессиональный уровень группы, стоящей за этой атакой, – это может означать, что «Маска» – это кампания, которая обеспечивается поддержкой какого-то государства.

Сам факт проведения этой вредоносной кампании ярко показывает, что существуют высокопрофессиональные киберпреступники, у которых есть опыт и ресурсы для разработки сложных вредоносных программ – в данном случае для кражи конфиденциальной информации. Это еще раз подтверждает, что вследствие того, что активность целевых атак относительно своих «особенных» жертв минимальна, они могут проходить «вне зоны действия радаров».

Также важно признать то, что вне зависимости от уровня сложности «Маски» атака начинается (как и в случае многих других целевых атак, известных ранее) с того, чтобы обманом заставить отдельных пользователей сделать что-либо, что поставит под угрозу безопасность организации, в которой они работают, – в данном случае это переход по ссылке.

В настоящее время все известные командные серверы, использованные в ходе «Маски», не работают. Однако в будущем вредоносная кампания может возобновиться.

ЧЕРВЬ И ЗМЕЯ

В начале марта в IT-сообществе шло широкое обсуждение кампании по кибершпионажу, известной под названием Turla (а также как Snake и Uroburos). По мнению исследователей из компании G-DATA, вредоносную программу, лежащую в основе этой кампании, могли создать российские спецслужбы. Исследование BAE Systems показало, что есть связь между Turla и вредоносной программой Agent.btz. Эта программа была создана еще в 2007 г. и применялась в 2008 г., чтобы заразить локальные сети, которые использовались в военных операциях США на Ближнем Востоке.

«Лаборатории Касперского» стало известно об этой серии целевых атак в ходе расследования инцидента, в который был вовлечен очень сложный руткит, который мы назвали «руткит Sun». Стало ясно, что Sun и Uroburos были одной и той же угрозой.

В данный момент мы все еще исследуем Turla – нам представляется, что он гораздо сложнее, чем это представлено в материалах, опубликованных на настоящий момент. Наш первичный анализ выявил некоторые интересные связи.

Agent.btz – это саморазмножающийся червь, способный распространяться через USB-флешки путем эксплуатации уязвимости, позволяющей флэшке запускаться с помощью autorun.inf.

Эта вредоносная программа смогла быстро распространиться по всему миру. Хотя на протяжении нескольких лет не было создано ни одного нового варианта червя, и хотя вышеупомянутая уязвимость была закрыта в новых версиях Windows, только за 2013 год Agent.btz был детектирован 13 832 раза в 107 странах мира!

Червь создает файл под названием thumb.dll на всех USB-флешках, присоединяемых к зараженному компьютеру (он содержит файлы winview.ocx, wmcache.nld и mssysmgr.ocx). Этот файл представляет собой контейнер для хранения украденных данных в случае, если эти данные нельзя прямо отослать по интернету на командный сервер, управляемый киберпреступниками. Если такая зараженная флешка затем подсоединяется к другому компьютеру, файл thumb.dll копируется на новый компьютер под именем mssysmgr.ocx.

По нашим оценкам, масштаб заражения этим червем, вооруженным вышеописанным функционалом, - это десятки тысяч флешек по всему миру, содержащих файл thumb.dll, созданный Agent.btz. В настоящее время большая часть вариантов этого зловреда распознаются защитными решениями «Лаборатории Касперского» под вердиктом «Worm.Win32.Orbina».

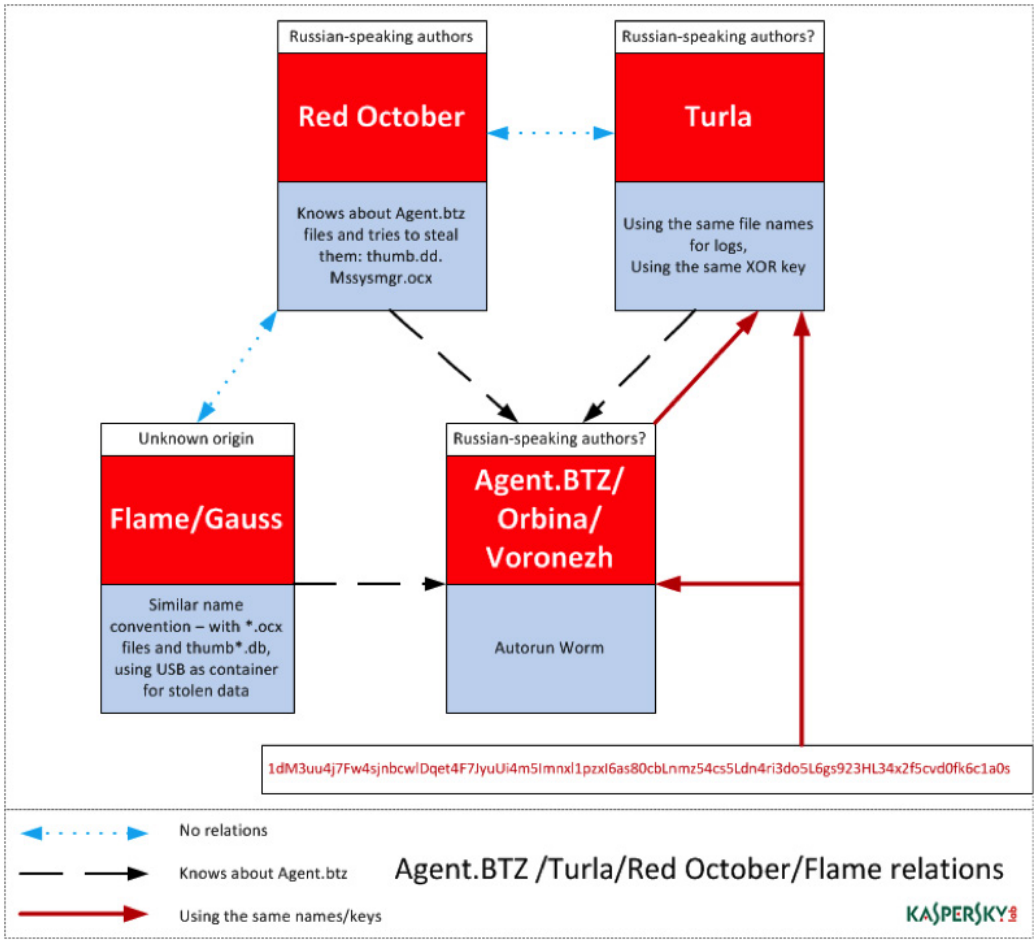
Конечно, Agent.btz – не единственная вредоносная программа, распространяющаяся через USB-флешки.

Модуль USB Stealer в Red October содержит список файлов, которые он ищет на USB-флешках, подсоединенных к зараженным компьютерам. Мы отметили, что в этот список входят файлы mysysmgr.ocx и thumb.dll, т.е. два файла, которые записываются на флешки червем Agent.btz.

Если заглянуть в чуть более отдаленное прошлое, то когда мы анализировали Flame и его близких родственников Gauss и miniFlame, то мы заметили в них сходные черты с Agent.btz. В частности, у них аналогичные принципы, по которым даются имена; особенно яркий пример – это использование расширения .ocx. Кроме того, было ясно, что и Gauss, и miniFlame знали о существовании файла thumb.dll и проверяли его наличие на USB-флешках.

Наконец, для журнала событий на зараженных компьютерах Turla использует те же имена файлов, что и Agent.btz: mswmpdat.tlb, winview.ocx и wmcache.nld. Совпадает и XOR-ключ, используемый для шифрования файлов журнала.

Все эти точки пересечения представлены ниже.



Итак, все, что мы знаем, – это то, что все эти вредоносные программы имеют некоторые сходства и точки пересечения. Понятно, что Agent.btz явился источником вдохновения для тех, что разрабатывал все прочие вредоносные программы из этого списка. Но мы не можем утверждать наверняка, что за всеми этими угрозами стоят одни и те же люди.

ИСТОРИИ ЗЛОВРЕДОВ: ЧИСТИМ ЛУК

Tor (аббревиатура от The Onion Router) – это программа, которая позволяет желающим анонимно подключаться к интернету. Программа существует уже довольно давно, но на протяжении многих лет ее использовали в основном эксперты и люди, увлеченные программированием. Однако в последние несколько месяцев число использующих Tor – в основном из соображений личной безопасности - резко выросло. Tor стал полезным решением для всех, кто по тем или иным причинам боится слежки и кражи персональных данных. А из нашего анализа стало понятно, что Tor привлекателен и для киберпреступников: они тоже ценят анонимность, которую эта программа обеспечивает.

В 2013 г. мы заметили, что киберпреступники стали активно использовать Tor для размещения инфраструктуры для своих вредоносных программ, а эксперты «Лаборатории Касперского» обнаружили различные вредоносные программы, использующие именно Tor. Исследование сетевых ресурсов Tor показало, что многие из них связаны с вредоносными программами – это командные серверы, панели администрирования и прочее. Размещая свои серверы в сети Tor, киберпреступники усложняют их распознавание, внесение их в черные списки и устранение.

Форумы и торговые площадки киберпреступников стали привычным делом в «обычном» интернете. Однако недавно появился еще и черный рынок на базе Tor. Все началось с пресловутого рынка Silk Road, вслед за которым появились десятки узкоспециальных рыночных площадок, на которых торгуют наркотиками, оружием и, конечно, вредоносным ПО.

Магазины краденых кредитных карт прочно обосновались на темной стороне интернета: продается краденая конфиденциальная информация, по которой можно вести поиск по широкому набору атрибутов: возможен поиск по стране, банку и т.д. Предлагаются и другие товары для мошенничеств с банковскими картами: дампы (информация, нелегально скопированная с магнитной полосы карт), скиммеры (оборудование для считывания информации с карт), прочее оборудование для кардинга.

Простота регистрации, рейтинги трейдеров, гарантированный сервис и удобный интерфейс – вот «джентльменский набор» черного рынка на базе Tor. В некоторых магазинах от торговцев требуют внести залог – определенную сумму денег – до начала торговли. Это является залогом того, что торговец представляет собой реальное лицо, а его сервисы качественны и не являются мошенническими.

Разработка Tor совпала по времени с возникновением анонимной криптовалюты биткойн. Практически все в сети Tor продается и покупается за биткойны. Соотнести биткойн-кошелек с реальным человеком практически невозможно, так что расчеты в «темном» интернете осуществляемые в биткойнах, обеспечивают практическую неуязвимость киберпреступников.

Весьма вероятно, что использование Tor и других анонимных сетей станет в интернете господствующей тенденцией: все большее число обычных людей, пользующихся интернетом, ищут способы защитить свою личную информацию. С другой стороны, анонимные сети привлекательны и для киберпреступников – с их помощью они могут скрывать действия создаваемого ими вредоносного ПО, заниматься торговлей на нелегальных ресурсах и отмывать свои нелегальные доходы. Мы полагаем, что популярность анонимных сетей среди киберпреступников только начинает набирать обороты.

СЕТЕВАЯ БЕЗОПАСНОСТЬ И УТЕЧКИ ДАННЫХ

ВЗЛЕТЫ И ПАДЕНИЯ БИТКОЙНА

Биткойн – это цифровая криптовалюта. Платежи в этой валюте проводятся по пиринговой модели: деньги перечисляются в виде цепочки цифровых сигнатур, которые представляют собой определенные суммы в биткойнах. Центрального контролирующего органа не существует, проценты за международные расчеты не взимаются. Эти два фактора содействовали популярности этой валюты как средства платежа. Общее описание криптовалюты биткойн и принципы ее работы описаны на нашей странице Kaspersky Daily.

По мере роста своей популярности биткойн стал интересовать киберпреступников как цель для атак.

В наших прогнозах на 2014 год мы предупреждали о будущих атаках на биткойн: «Атаки на биткойн-пулы, биржи и пользователей Bitcoin станут одной из самых громких тем года». Там же говорилось, что такие атаки «будут пользоваться наибольшей популярностью у киберпреступников, поскольку при таких атаках соотношение затрат и прибыли оптимальное».

Уже было немало случаев, подтвердивших наш прогноз. Mt.Gox – один из крупнейших биткойн-обменников – был отключен 25 февраля. Этому предшествовал месяц, полный проблем для торговой площадки, – курс биткойна на сайте резко упал. Появились сообщения о том, что несостоятельность этого биткойн-обменника наступила после взлома, приведшего к краже 774 408 биткойнов, что эквивалентно примерно 350 миллионам долларов на момент закрытия обменника. Похоже, главной проблемой в этом случае стала гибкость протокола биткойн-транзакций: при некоторых условиях протокол позволяет атакующей стороне назначать одной и той же транзакции несколько различных идентификаторов; в результате кажется, что транзакция не произошла. Здесь вы можете ознакомиться с нашей оценкой событий, произошедших при крахе Mt.Gox. Уязвимость, связанная с гибкостью протокола, теперь закрыта. Естественно, атаки были не только на Mt.Gox; под удар попали и другие провайдеры виртуальных банковских сервисов – мы говорили об этом в конце прошлого года. Рост популярности виртуальных валют наверняка означает, что в будущем атаки на них продолжатся.

Атакам подвержены не только обменники виртуальных валют. Под ударом могут оказаться и сами люди, использующие криптовалюту. В середине марта были взломаны личный блог и учетная запись Reddit гендиректора Mt.Gox Марка Карпелеса. Эти аккаунты были использованы для размещения файла MtGox2014Leak.zip. Предполагалось, что в этом файле содержались ценные дампы баз данных, а также специальное ПО для удаленного доступа к данным Mt.Gox. На деле оказалось, что файл содержал вредоносное ПО для поиска и кражи файлов с биткойн-кошельками. Наш анализ зловреда доступен здесь. Перед вами – яркий пример того, как киберпреступники используют человеческий интерес к последним новостям для продвижения вредоносного ПО.

В связи со всеми этими атаками встает очень важный вопрос. Как те из нас, кто пользуется какой-либо криптовалютой, обеспечат свою безопасность в среде, в которой – в отличие от реальных валют – не действуют никакие внешние стандарты и нормативные положения? Наш совет – храните свои биткойны в опенсорсном офлайн-клиенте (а не в сервисах онлайн-бирж с неизвестным уровнем безопасности), а если у вас много биткойнов – то в кошельке на компьютере, не подключенном к интернету. Кроме того, советуем использовать по возможности сложные парольные фразы к биткойн-кошелькам, ну и иметь на компьютере достойный защитный продукт.

Спамеры тоже охотно используют методы социальной инженерии, чтобы завлечь людей в мошеннические схемы. Они воспользовались повышением курса биткойнов в первом квартале года (еще до краха Mt.Gox) и постарались сделать деньги, сыграв на желании людей быстро обогатиться. Как мы отмечали в феврале, в ходу у спамеров было несколько тем, связанных с биткойном, среди них предложения поделиться «секретами от миллионера» по поводу того, как стать богатым, вкладывая деньги в биткойны; а также предложения поучаствовать в биткойн-лотерее.

КАК ИСПОЛЬЗОВАТЬ ХОРОШИЙ СОФТ В ПЛОХИХ ЦЕЛЯХ

На Саммите вирусных аналитиков-2014 мы в общих чертах рассказали, как некоторые технологии защиты от кражи, которые внедрены в прошивку популярных моделей ноутбуков и некоторых стационарных компьютеров, могут стать мощным оружием в руках киберпреступников.

Наше расследование началось в связи с тем, что один сотрудник «Лаборатории Касперского» столкнулся на своем личном лэптопе с неоднократными сбоями системных процессов. Анализ журнала событий и дампа памяти вскрыл, что сбои происходили из-за нестабильной работы модулей identprv.dll и wceprv.dll, которые были загружены в адресное пространство одного из главных процессов системных сервисов (svchost.exe). Эти модули были созданы легальным производителем Absolute Software и являются составной частью программного продукта Absolute Computrace.

Наш коллега утверждал, что он не устанавливал этот программный продукт, и даже не знал, что он присутствовал на ноутбуке. Это нас встревожило, поскольку, как сообщается в white paper Absolute Software, установка должна производиться владельцем компьютера или обслуживающей его IT-службой. Кроме того, в отличие от большинства предустановленных программ, которые владелец компьютера может насовсем удалить или заблокировать, Computrace сделан так, что сохраняется на компьютере при профессиональной очистке системы и даже при замене жесткого диска. Более того, мы не могли проигнорировать это явление как однократное и случайное, потому что обнаружили указания на то, что Computrace исполнялся на личных компьютерах некоторых наших аналитиков и некоторых корпоративных машинах. В результате мы решили провести подробное расследование.

Когда мы только взглянули на Computrace, мы решили было, что это был зловред, – его разработчики использовали очень много приемов, популярных в сегодняшних вредоносных программах: применяются специфические технологии отладки и противодействия обратному инжинирингу, код внедряется в память других процессов, происходит скрытый обмен данными, производятся программные вставки в системные файлы на диске, конфигурационные файлы шифруются, а Windows-исполняемый файл выгружается прямо из BIOS/прошивки. По этой причине этот программный продукт в прошлом детектировался как вредоносное ПО; однако сегодня большинство производителей защитных решений внесли исполняемые файлы Computrace в свои белые списки.

Мы считаем, что Computrace был разработан с добрыми намерениями. Тем не менее, наше исследование показало, что уязвимости, существующие в этом ПО, позволяют киберпреступникам использовать его злонамеренно. На наш взгляд, если инструмент такой мощный, то совершенно необходимо, чтобы в нем были встроены очень жесткие средства аутентификации и шифрования. Мы не обнаружили указаний на то, что на подвергшихся нашему анализу компьютерах скрытно активировались модули Computrace. Однако ясно, что существует много компьютеров с активированными агентами Computrace. Мы считаем, что на производителе программного продукта, Absolute Software, лежит ответственность за то, чтобы сообщить о программе всем этим пользователям и объяснить, как деактивировать это ПО в случае, если они не хотят его использовать. В противном случае эти «подвисшие» агенты будут продолжать незаметно работать и создавать возможность удаленной эксплуатации.

МОБИЛЬНЫЕ УГРОЗЫ

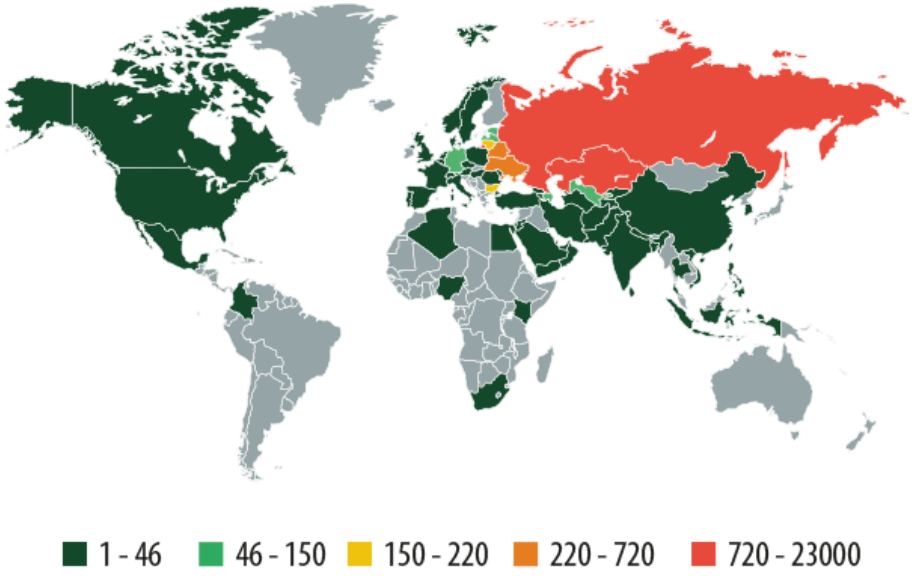
В этом квартале доля угроз под Android превысила 99% от всех мобильных вредоносных программ. В течение квартала было обнаружено:

- > 1 258 436 установочных пакетов,
- > 110 324 новых мобильных вредоносных программ,
- > 1 182 новых мобильных банковских троянцев.

МОБИЛЬНЫЕ БАНКОВСКИЕ ТРОЯНЦЫ

Если на начало квартала нам был известен 1321 уникальный исполняемый файл банковских мобильных банкеров, то на конец квартала их стало уже 2503. Таким образом, за квартал поголовье банковских троянцев увеличилось почти вдвое.

По-прежнему наиболее актуальна эта угроза в России, Казахстане, Белоруссии и на Украине:



География мобильных банковских угроз в первом квартале 2014

ТОП 10 СТРАН, АТАКУЕМЫХ БАНКОВСКИМИ ТРОЯНЦАМИ:

	СТРАНА	% АТАК
1	**Россия**	88,85%
2	**Казахстан**	3,00%
3	**Украина**	2,71%
4	**Белоруссия**	1,18%
5	**Литва**	0,62%
6	**Болгария**	0,60%
7	**Азербайджан**	0,54%
8	**Германия**	0,39%
9	**Латвия**	0,34%
10	**Узбекистан**	0,30%

Один из банковских троянцев Faketoken – по итогам квартала вошел в TOP 20 детектируемых «Лабораторией Касперского» мобильных вредоносных программ. Этот зловред ворует mTAN и работает в паре с компьютерными банковскими троянцами. Компьютерные троянцы во время сессии онлайн-банкинга, используя веб-инжект, внедряют на загруженную в браузер страницу банка требование скачать Android-приложение, которое якобы необходимо для безопасного осуществления транзакции, и ссылку на Faketoken. После того, как мобильный зловред оказывается на смартфоне пользователя, злоумышленники с помощью компьютерных троянцев получают доступ к банковскому аккаунту пользователя, а Faketoken позволяет им заполучить mTAN и перевести деньги пользователя на свои счета.

Мы неоднократно писали о том, что большинство мобильных банкеров создаются и изначально используются в России, но потом злоумышленники могут их использовать и в других странах. Faketoken – одна из таких программ. В первом квартале 2014 года были зафиксированы атаки этого зловреда на пользователей в 55 странах, в том числе в Германии, Швеции, Франции, Италии, Великобритании и в США.

НОВИНКИ ОТ ВИРУСОПИСАТЕЛЕЙ

БОТ, УПРАВЛЯЕМЫЙ ЧЕРЕЗ TOR

Анонимная сеть Tor, построенная на сети прокси-серверов, обеспечивает анонимность пользователя и позволяет размещать в доменной зоне .onion «анонимные» сайты, доступные только в Tor. В феврале мы обнаружили первый Android-троянец, который использует в качестве C&C домен в псевдо-зоне .onion.

Backdoor.AndroidOS.Torec.a представляет собой изменённый популярный Tor-клиент Orbot, в который злоумышленники добавили свой код. Отметим, что для того, чтобы Backdoor.AndroidOS.Torec.a мог использовать Tor, потребовалось гораздо больше кода, чем для его собственного функционала.

Троянец может получать с C&C следующие команды:

- начать/закончить перехват входящих SMS;
- начать/закончить кражу входящих SMS;
- сделать USSD запрос;
- отправить на C&C данные о телефоне (телефонный номер, страна, IMEI, модель, версия OS);
- отправить на C&C список установленных на мобильном устройстве приложений;
- отправить SMS на номер, указанный в команде.

Зачем злоумышленникам понадобилась анонимная сеть? Ответ прост: C&C, размещенный в сети Tor, невозможно закрыть. Отметим, что такой подход создатели Android-троянцев переняли у вирусописателей, создающих Windows-зловреды.

КРАЖИ С ЭЛЕКТРОННЫХ КОШЕЛЬКОВ

Злоумышленники постоянно ищут новые способы кражи денег при помощи мобильных троянцев. В марте мы обнаружили троянец Trojan-SMS.AndroidOS.Waller.a, который, помимо

стандартных для Trojan-SMS действий, способен воровать деньги с электронных кошельков QIWI-Wallet владельцев зараженных смартфонов.

Получив соответствующую команду с C&C, троянец проверяет баланс счета электронного кошелька QIWI-Wallet. Для этого он отправляет SMS на соответствующий номер системы QIWI. Полученные в ответ SMS троянец перехватывает и переправляет их своим хозяевам.

Если у владельца зараженного устройства есть счет QIWI-Wallet, и троянец получает информацию о положительном балансе электронного кошелька, то вредоносная программа может переводить деньги со счета пользователя на указанный злоумышленниками счет QIWI Wallet. Для этого по команде хозяев троянец отправляет на специальный номер системы QIWI SMS, в котором указаны номер кошелька злоумышленников и сумма перевода.

Пока троянец атакует только российских пользователей. Однако злоумышленники с его помощью могут воровать деньги и у пользователей других стран, где представлены электронные кошельки с возможностью управления с помощью SMS.

НЕПРИЯТНЫЕ НОВОСТИ

В первом квартале 2014 года был обнаружен троянец для iOS. Данная вредоносная программа представляет собой плагин для Cydia Substrate, популярного фреймворка для рутованых/взломанных устройств. Во многих партнерских программах разработчики приложений, разместившие в своих приложениях рекламные модули, получают деньги за показанную рекламу. Обнаруженный троянец подменяет в некоторых рекламных модулях ID создателей программы на ID злоумышленников. В результате все деньги за показанную рекламу попадают к злоумышленникам.

Эксперт из Турции обнаружил уязвимости, эксплуатация которых приводит к DOS устройства и его последующей перезагрузке. Суть уязвимости заключается в том, что можно сформировать Android-приложение с AndroidManifest.xml, содержащим в любом поле name очень большое количество данных. (AndroidManifest.xml – это специальный файл, который есть в каждом Android-приложении. В этом файле содержатся сведения о приложении, в том числе разрешения на доступ к системным функциям, указатели на обработчики различных событий

и тд.) Установка созданного приложения произойдет без проблем, но, например, при вызове activity с таким именем произойдет сбой в устройстве. Как пример, может быть сформирован обработчик входящих SMS с неправильным именем, и после получения любого SMS телефоном станет невозможно пользоваться. Мобильное устройство начнет постоянно перезагружаться, и у пользователя останется только одна возможность – откатить прошивку. Что приведет к потере пользовательских данных на устройстве.

ВРЕДОНОСНЫЙ СПАМ

Один из стандартных способов распространения мобильных зловредов – вредоносный спам. Особенно этот метод популярен у злоумышленников, с помощью мобильных троянцев ворующих деньги с банковских счетов пользователей.

Вредоносное спамовое SMS-сообщение, как правило, содержит либо предложение скачать приложение со ссылкой на зловред, либо ссылку на сайт, с которого распространяется вредоносная программа, на который пользователя заманивают под тем или иным предлогом. Как и в случае с почтовым вредоносным спамом, для привлечения внимания пользователей активно используется социальная инженерия.

ОЛИМПИЙСКИЙ СПАМ

Олимпийские игры – событие, несомненно, значимое. И злоумышленники воспользовались интересом к ним со стороны пользователей.

В феврале мы зарегистрировали спам-рассылку SMS сообщений со ссылкой якобы на трансляцию соревнований на Олимпиаде. Если неосторожный пользователь кликал по ссылке, на его смартфон пытался загрузиться троянец, детектируемый нами как HEUR:Trojan-SMS.AndroidOS.FakeInst.fb.

Этот троянец способен по команде злоумышленников отправлять SMS на номер одного из крупных российских банков и переводить деньги с банковского на мобильный счет владельца зараженного смартфона. А с мобильного счета жертвы злоумышленники могут переводить

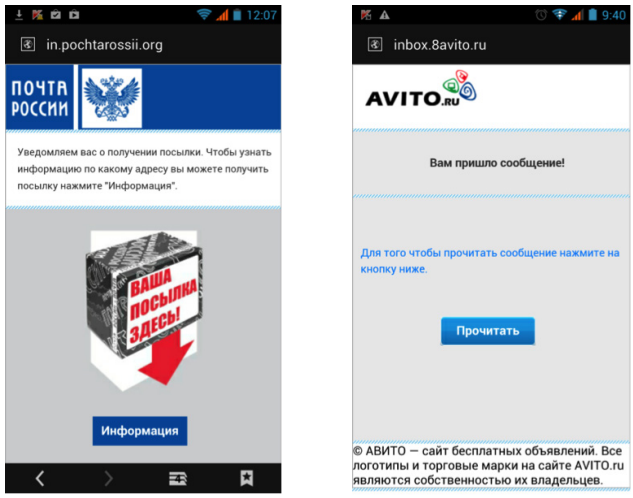
деньги на свои электронные кошельки. При этом все сообщения от банка о переводе денег будут скрыты от пользователя.

СПАМ СО ССЫЛКОЙ НА ВРЕДОНОСНЫЕ САЙТЫ

Злоумышленники, распространяющие троянца Opfake, рассылали SMS-спам со ссылкой на специально созданные вредоносные сайты.

В одном из спамовых SMS сообщалось, что пользователю пришла посылка, и ссылка вела на сайт, замаскированный под ресурс Почты России:

В других рассылках злоумышленники использовали популярность российского сайта бесплатных объявлений Avito.ru. SMS содержали сообщения «Вы получили предложение на ваше объявление» или «Появился покупатель на ваш товар» и ссылки, которые вели на поддельную страницу Avito.ru.



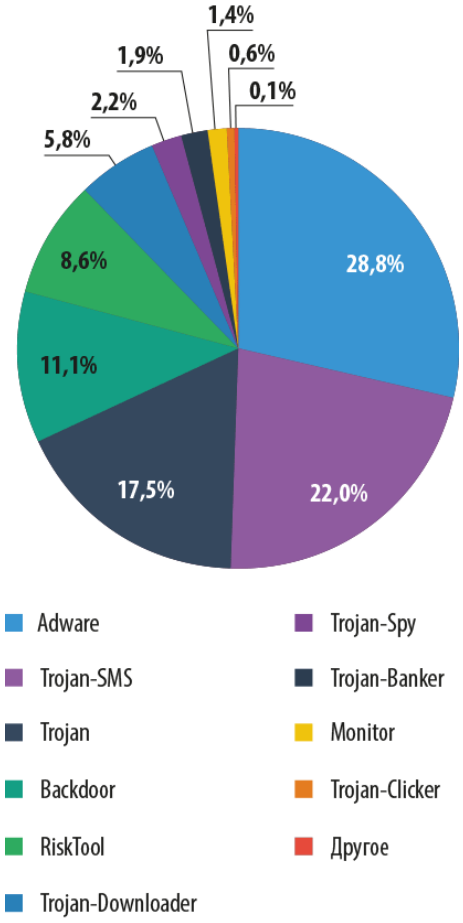
Поддельные вредоносные страницы

Если пользователь кликал по ссылкам на фальшивых сайтах, на его смартфон пытался загрузиться троянец Trojan-SMS.AndroidOS.Opfake.a. Помимо рассылки платных SMS, эта вредоносная программа используется для распространения других мобильных зловредов, в частности, многофункционального Backdoor.AndroidOS.Obad.a.

Социальная инженерия всегда была опасным инструментом в руках злоумышленников. Пользователям надо быть внимательными и, как минимум, не переходить по ссылкам, полученным от неизвестных отправителей. В таких случаях всегда есть риск попасть в ловушку злоумышленников и, как следствие, потерять немалые деньги.

СТАТИСТИКА

РАСПРЕДЕЛЕНИЕ ПО ТИПАМ МОБИЛЬНЫХ ЗЛОВРЕДОВ



Распределение по типам мобильных зловредов, первый квартал 2014 года

В первом квартале 2014 года впервые на первом месте оказались рекламных модули (Adware), единственный функционал которых - показывать навязчивую рекламу. Отметим, что такого рода модули особенно популярны в Китае.

Долгое время преобладающие среди мобильных зловредов SMS-троянцы сместились на второе место, за квартал их доля уменьшилась с 34% до 22%. Однако эта категория программ по-прежнему преобладает в TOP 20 детектируемых мобильных вредоносных программ.

TOP 20 МОБИЛЬНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

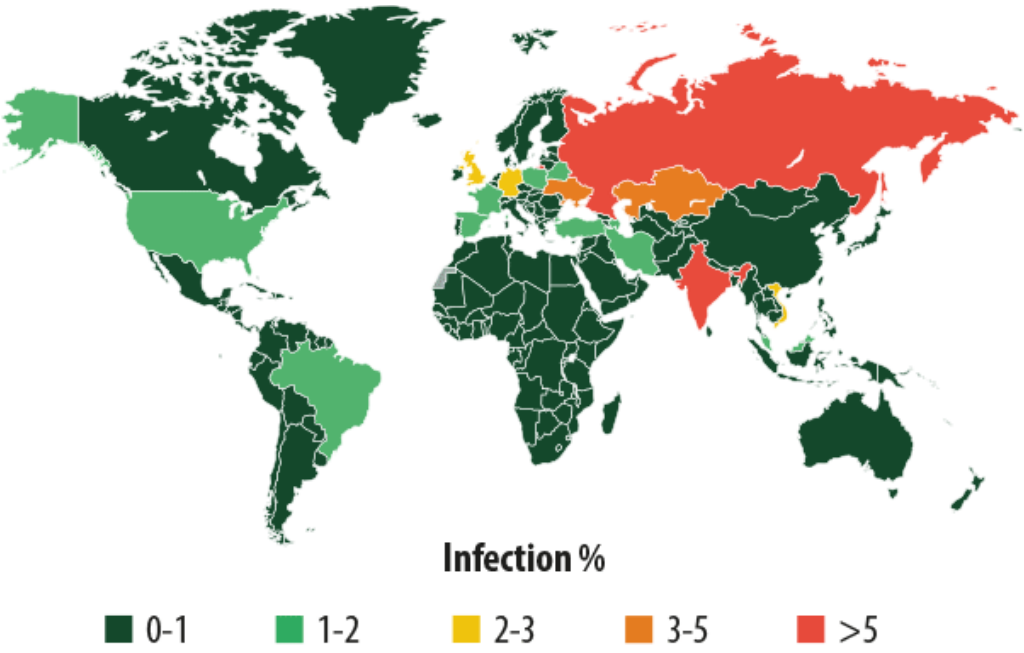
	НАЗВАНИЕ	% АТАК
1	Trojan-SMS.AndroidOS.Stealer.a	22,77%
2	RiskTool.AndroidOS.MimobSMS.a	11,54%
3	Trojan-SMS.AndroidOS.OpFake.bo	11,30%
4	RiskTool.AndroidOS.Mobogen.a	10,50%
5	DangerousObject.Multi.Generic	9,83%
6	Trojan-SMS.AndroidOS.FakeInst.a	9,78%
7	Trojan-SMS.AndroidOS.OpFake.a	7,51%
8	Trojan-SMS.AndroidOS.Erop.a	7,09%
9	Trojan-SMS.AndroidOS.Agent.u	6,45%
10	Trojan-SMS.AndroidOS.FakeInst.ei	5,69%
11	Backdoor.AndroidOS.Fobus.a	5,30%
12	Trojan-SMS.AndroidOS.FakeInst.ff	4,58%
13	Trojan-Banker.AndroidOS.Faketoken.a	4,48%
14	AdWare.AndroidOS.Ganlet.a	3,53%
15	Trojan-SMS.AndroidOS.Agent.ao	2,75%
16	AdWare.AndroidOS.Viser.a	2,31%
17	Trojan-SMS.AndroidOS.Agent.dr	2,30%
18	Trojan-SMS.AndroidOS.Agent.fk	2,25%
19	RiskTool.AndroidOS.SMSreg.dd	2,12%
20	RiskTool.AndroidOS.SMSreg.eh	1,87%

Значимый вклад в увеличение числа новых мобильных зловредов внесли в первом квартале новые модификации троянца Trojan-SMS.AndroidOS.Stealer.a. Ничем особенным этот зловред не отличается, у него стандартный для SMS-троянцев функционал, однако он занимает первое место в TOP 20 детектируемых угроз.

Разумеется, прошлогодние лидеры Opfake.bo и Fakeinst.a не собираются сдавать позиции и по-прежнему активно атакуют мобильных пользователей, что выливается в нескончаемый поток новых вредоносных установочных пакетов.

Отметим, что в TOP 20 детектируемых «Лабораторией Касперского» мобильных вредоносных программ впервые вошел и банковский троянец Faketoken (13-е место).

ГЕОГРАФИЯ УГРОЗ



Карта попыток заражений мобильными зловредами
(процент от всех атакованных уникальных пользователей)

ТОР 10 АТАКУЕМЫХ СТРАН

	СТРАНА	% АТАК
1	**Россия**	48,90%
2	**Индия**	5,23%
3	**Казахстан**	4,55%
4	**Украина**	3,27%
5	**Великобритания**	2,79%
6	**Германия**	2,70%
7	**Вьетнам**	2,44%
8	**Малайзия**	1,79%
9	**Испания**	1,58%
10	**Польша**	1,54%

СТАТИСТИКА

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN) как результат работы различных компонентов защиты от вредоносных программ. Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их передачу. В глобальном обмене информацией о вредоносной активности принимают участие миллионы пользователей продуктов «Лаборатории Касперского» из 213 стран и территорий мира.

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ (АТАКИ ЧЕРЕЗ WEB)

Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями (например, форумы), а также взломанные легитимные ресурсы.

ТОР 20 ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ В ИНТЕРНЕТЕ

В первом квартале 2014 года нашим веб-антивирусом было задетектировано **29 122 849** уникальных вредоносных объектов (скрипты, веб-страницы, эксплойты, исполняемые файлы и т.д.).

Из всех вредоносных программ, участвовавших в интернет-атаках на компьютеры пользователей, мы выделили 20 наиболее активных. На них пришлось 99,8% всех атак в интернете.

	НАЗВАНИЕ*	% ОТ ВСЕХ АТАК**
1	**Malicious URL**	81,73%
2	**Trojan.Script.Generic**	8,54%
3	**AdWare.Win32.BetterSurf.b**	2,29%
4	**Trojan-Downloader.Script.Generic**	1,29%
5	**Trojan.Script.Iframer**	1,21%
6	**AdWare.Win32.MegaSearch.am**	0,88%
7	**Trojan.Win32.AntiFW.b**	0,79%
8	**AdWare.Win32.Agent.ahbx**	0,52%
9	**AdWare.Win32.Agent.aiyc**	0,48%
10	**Trojan.Win32.Generic**	0,34%
11	**AdWare.Win32.Yotoon.heur**	0,28%
12	**Trojan.Win32.Agent.aduro**	0,23%
13	**Adware.Win32.Amonetize.heur**	0,21%
14	**Trojan-Downloader.Win32.Generic**	0,21%
15	**Trojan-Clicker.JS.FbLiker.k**	0,18%
16	**Trojan.JS.Iframe.ahk**	0,13%
17	**AdWare.Win32.Agent.aiwa**	0,13%
18	**Exploit.Script.Blocker**	0,12%
19	**AdWare.MSIL.DomaIQ.pef**	0,12%
20	**Exploit.Script.Generic**	0,10%

** Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.*

*** Процент от всех веб-атак, которые были зафиксированы на компьютерах уникальных пользователей.*

Традиционно в TOP 20 по большей части представлены вердикты, которые присваиваются объектам, использующимся в drive-by атаках, а также рекламным программам. Количество позиций с вердиктами для рекламных программ увеличилось по сравнению с прошлым кварталом с 7 до 9.

Среди программ в рейтинге стоит выделить Trojan.Win32.Agent.aduro (12-е место). Данная программа распространяется с веб-сайтов, на которых пользователю предлагают скачать плагин браузера, помогающий совершать онлайн-покупки.

После клика по кнопке “Download”, на компьютер пользователя пытается загрузиться Trojan.Win32.Agent.aduro. Задача троянца – скачать предлагаемый рекламный плагин, а вместе с ним тайком от пользователя он загружает программу для майнинга криптовалюты Litecoin. В результате злоумышленники будут использовать для генерации криптовалюты для своего кошелька ресурсы зараженной машины пользователя.

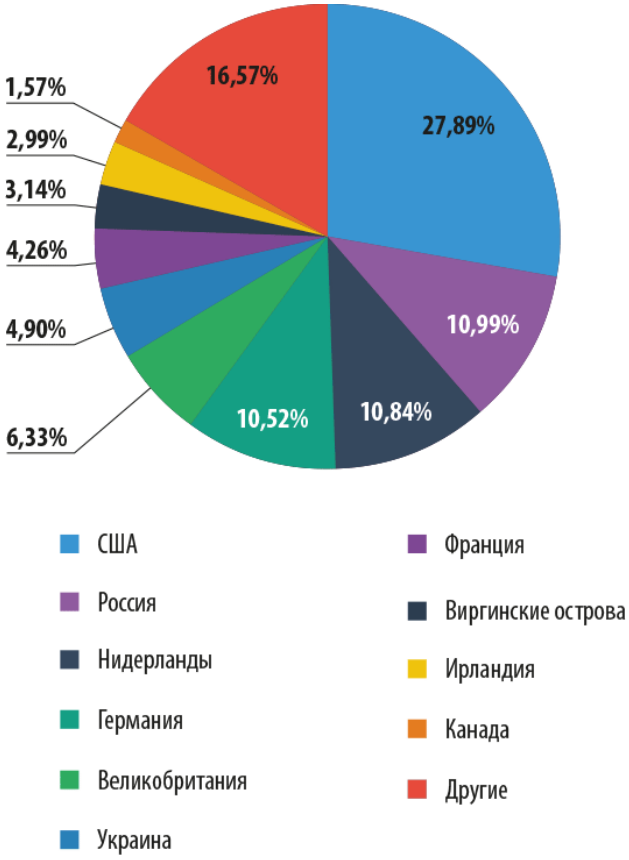
Также интересен вредоносный скрипт Trojan-Clicker.JS.FbLiker.k (15-е место), который встречается в основном на вьетнамских сайтах с различным развлекательным контентом и ресурсах, на которых пользователю предлагается скачать фильмы и программы. Когда пользователь заходит на такой сайт, скрипт имитирует нажатие посетителем кнопки Like на определенной странице в социальной сети Facebook. В результате эта страница на Facebook может отображаться как понравившаяся во френдленте друзей пользователя и в профиле пользователя. Также количество «лайков» у определенной страницы влияет на ее выдачу в поиске Facebook.

СТРАНЫ - ИСТОЧНИКИ ВЕБ-АТАК: TOP 10

Данная статистика показывает распределение по странам источников заблокированных антивирусом веб-атак на компьютеры пользователей (веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т.д.). Отметим, что каждый уникальных хост мог быть источником одной и более веб-атак.

Для определения географического источника веб-атак использовалась методика сопоставления доменного имени с реальным IP-адресом, на котором размещен данный домен, и установление географического местоположения данного IP-адреса (GEOIP).

В первом квартале 2014 года решения «Лаборатории Касперского» отразили 353 216 351 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира. 83,4% нотификаций о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира. Это на 0,3% меньше, чем в предыдущем квартале.



Распределение по странам источников веб-атак, первый квартал 2014

Этот рейтинг за последние месяцы изменился незначительно. Отметим, что 39% веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США и России.

СТРАНЫ, В КОТОРЫХ ПОЛЬЗОВАТЕЛИ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЗАРАЖЕНИЯ ЧЕРЕЗ ИНТЕРНЕТ

Чтобы оценить степень риска заражения через интернет, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали, сколько уникальных пользователей продуктов «Лаборатории Касперского» в каждой стране сталкивались со срабатыванием веб-антивируса. Полученные данные являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

	СТРАНА*	% УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ**
1	**Вьетнам**	51,44%
2	**Россия**	49,38%
3	**Казахстан**	47,56%
4	**Армения**	45,21%
5	**Монголия**	44,74%
6	**Украина**	43,63%
7	**Азербайджан**	42,64%
8	**Белоруссия**	39,40%
9	**Молдова**	38,04%
10	**Киргизия**	35,87%
11	**Таджикистан**	33,20%
12	**Грузия**	32,38%
13	**Хорватия**	31,85%
14	**Катар**	31,65%
15	**Алжир**	31,44%
16	**Турция**	31,31%
17	**Литва**	30,80%
18	**Греция**	30,65%
19	**Узбекистан**	30,53%
20	**Испания**	30,47%

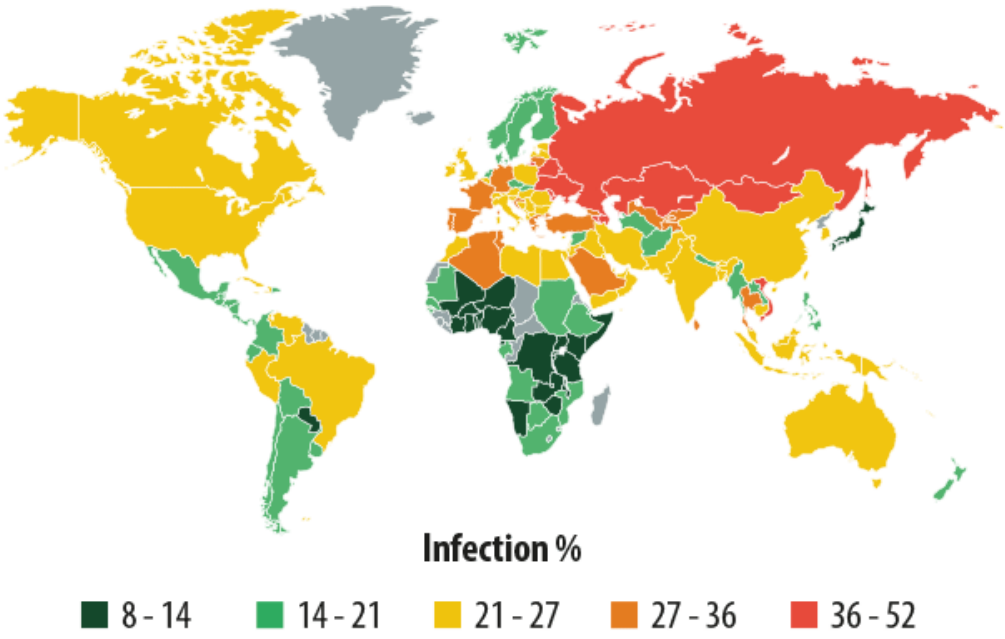
Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

**При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).*

***Процент уникальных пользователей, подвергшихся веб-атакам, от всех уникальных пользователей продуктов ЛК в стране.*

В первом квартале 2014 года в этом рейтинге сменился лидер: первое место занял Вьетнам, где веб-атакам подверглись 51,4% пользователей. Новым участником рейтинга стала Монголия, которая заняла сразу 5-ю строчку рейтинга с показателем 44,7% атакованных пользователей. Остальные позиции в первой десятке стран рейтинга традиционно занимают Россия и страны бывшего СНГ.

Среди самых безопасных при серфинге в интернете стран, Сингапур (10,5%), Япония (13,2%), Швеция (14,5%), ЮАР (15,6%), Тайвань (16,1%), Дания (16,4%), Финляндия (16,8%), Нидерланды (17,7%), Норвегия (19,4%).



*процент от всех атакованных уникальных пользователей

В среднем в течение квартала в мире 33,2% компьютеров пользователей интернета хотя бы раз подвергались веб-атаке.

ЛОКАЛЬНЫЕ УГРОЗЫ

Исключительно важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают объекты, которые проникли на компьютеры не через интернет, почту или сетевые порты.

В этом разделе мы анализируем статистические данные, полученные на основе работы антивируса, сканирующего файлы на жестком диске в момент их создания или обращения к ним, и данные по сканированию различных съемных носителей информации.

В первом квартале 2014 года наши антивирусные решения заблокировали 645 809 230 вирусных атак на компьютерах пользователей. Всего в данных инцидентах было зафиксировано 135 227 372 уникальных вредоносных и потенциально нежелательных объектов.

ДЕТЕКТИРУЕМЫЕ ОБЪЕКТЫ, ОБНАРУЖЕННЫЕ НА КОМПЬЮТЕРАХ ПОЛЬЗОВАТЕЛЕЙ: TOP 20

	НАЗВАНИЕ	% АТАКОВАННЫХ УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ*
1	**DangerousObject.Multi.Generic**	20,37%
2	**Trojan.Win32.Generic**	18,35%
3	**AdWare.Win32.Agent.ahbx**	12,29%
4	**Trojan.Win32.AutoRun.gen**	7,38%
5	**AdWare.Win32.BetterSurf.b**	6,67%
6	**Adware.Win32.Amonetize.heur**	5,87%
7	**Virus.Win32.Sality.gen**	5,78%
8	**Worm.VBS.Dinihou.r**	5,36%
9	**AdWare.Win32.Yotoon.heur**	5,02%
10	**Trojan-Dropper.Win32.Agent.jkcd**	4,94%
11	**Worm.Win32.Debris.a**	3,40%
12	**Trojan.Win32.Starter.lgb**	3,32%
13	**Exploit.Java.Generic**	3,00%
14	**AdWare.Win32.Skyli.a**	2,80%
15	**Trojan.Win32.AntiFW.b**	2,38%
16	**Virus.Win32.Nimnul.a**	2,23%

17	**Trojan.WinLNK.Runner.ea**	2,22%
18	**AdWare.Win32.DelBar.a**	2,21%
19	**AdWare.Win32.BrainInst.heur**	2,11%
20	**Worm.Script.Generic**	2,06%

Данная статистика представляет собой детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

**Процент уникальных пользователей, на компьютерах которых антивирус детектировал данный объект, от всех уникальных пользователей продуктов ЛК, у которых происходило срабатывание антивируса.*

Традиционно в данном рейтинге представлены вердикты, которые присваиваются рекламным программам, червям, распространяющимся на съемных носителях, и вирусам.

Доля вирусов в TOP 20 продолжает стабильно, но медленно падать. В первом квартале вирусы представлены вердиктами Virus.Win32.Sality.gen и Virus.Win32.Nimnul.a с общим показателем 8%, для сравнения в четвертом квартале этот показатель был 9,1%.

Червь Worm.VBS.Dinihou.r, представляющий собой VBS-скрипт, появился в конце прошлого года, а в рейтинг попал впервые (8-е место). Этот червь распространяется, в частности, с помощью спама. Червь реализует широкий функционал полноценного бэкдора, начиная от запуска командной строки, заканчивая загрузкой на сервер заданного файла. Кроме того, он и инфицирует подключенные к компьютеру USB-накопители.

СТРАНЫ, В КОТОРЫХ КОМПЬЮТЕРЫ ПОЛЬЗОВАТЕЛЕЙ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЛОКАЛЬНОГО ЗАРАЖЕНИЯ

	СТРАНА*	% УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ**
1	**Вьетнам**	60,30%
2	**Монголия**	56,65%
3	**Непал**	54,42%
4	**Алжир**	54,38%
5	**Йемен**	53,76%
6	**Бангладеш**	53,63%
7	**Египет**	51,30%
8	**Ирак**	50,95%
9	**Афганистан**	50,86%

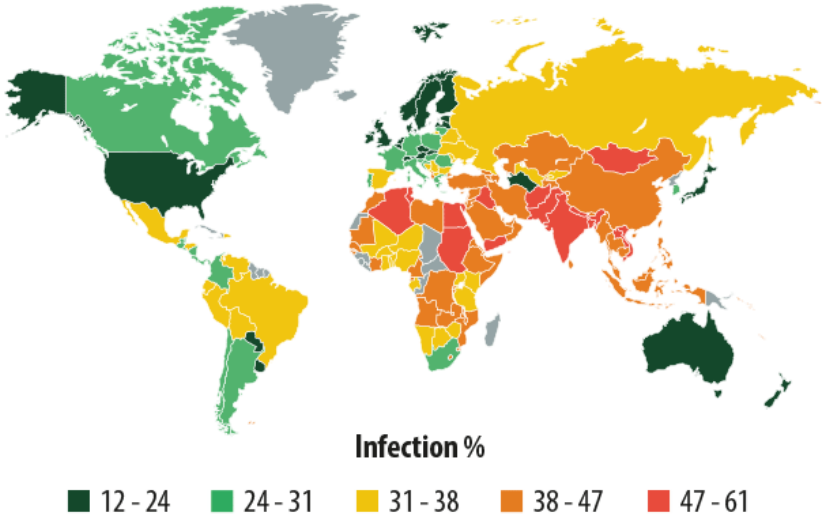
10	Пакинстан	49,79%
11	Индия	49,02%
12	Судан	48,76%
13	Тунис	48,47%
14	Джибути	48,27%
15	Лаос	47,40%
16	Сирия	46,94%
17	Мьянма	46,92%
18	Камбоджа	46,91%
19	Марокко	46,01%
20	Индонезия	45,61%

Настоящая статистика основана на детектирующих вердиктах модуля антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных. Учитывались вредоносные программы, найденные непосредственно на компьютерах пользователей или же на съемных носителях, подключенных к компьютерам — флешках, картах памяти фотоаппаратов, телефонов, внешних жестких дисках.

**При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (меньше 10 тысяч).*

***Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.*

Страны Африки, Ближнего Востока и Юго-Восточной Азии стабильно занимают все позиции в этом рейтинге. Как и в предыдущем квартале, лидирует в нем Вьетнам, Монголия осталась на втором месте. Непал поднялся с четвертого на третье место, а Бангладеш сместился с третьего на шестое. Новичком в рейтинге выступает Марокко.



*процент от всех атакованных уникальных пользователей

В число самых безопасных по уровню локального заражения стран попали: Япония (12,6%), Швеция (15%), Финляндия (15,3%), Дания (15,4%), Сингапур (18,2%), Нидерланды (19,1%), Чехия (19,5%).

В среднем в мире хотя бы раз в течение года локальные угрозы были зафиксированы на 34,7% компьютеров пользователей.